IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

ADAM MATOT,

Plaintiff,

v.

CH et al.,

Defendants.

Civ. No. 6:13-cv-153-MC

OPINION AND ORDER

MCSHANE, Judge:

Plaintiff brings this action seeking damages and equitable relief for alleged violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, defamation, negligent supervision, and parental liability pursuant to Oregon Revised Statute § 30.765. Defendant, Gary Hill, filed this motion to dismiss for lack of subject matter jurisdiction (#14). Defendant, S.A., filed this motion for entry of a limited judgment and injunction (#25). Magistrate Judge Thomas M. Coffin filed two Findings and Recommendations (F & R) in response to defendants' motions (#14) and (#25), and these matters are now before this court. *See* 28 U.S.C. § 636(b)(1)(B) (2012); Fed. R. Civ. P. 72(b).

Because no objections to either F & R were filed, this court reviews only the legal principles *de novo*. *United States v. Reyna-Tapia*, 328 F.3d 1114, 1121 (9th Cir. 2003) (en banc); *see also United States v. Bernhardt*, 840 F.2d 1441, 1445 (9th Cir. 1988). Upon review, this court finds find no error in F & R (#27) or F & R (#29) and ADOPTs both in full. Defendant Gary Hall's motion to dismiss for lack of subject matter jurisdiction (#14) is GRANTED and

defendant S.A.'s motion for entry of a limited judgment and injunction (#25) is DENIED consistent with this opinion.

DISCUSSION

Plaintiff's CFAA claim rests on defendants' alleged use "without authorization" of social media services (e.g., Facebook and Twitter) and defendants' alleged use "exceed[ing] authorized access" of social media services, i.e., defendants' violation of the terms of use of the particular social media service. As indicated by Judge Coffin in F & R (#27), a mere violation of a use restriction, i.e., "exceed[ing] authorized access," is not actionable under the CFAA in the Ninth Circuit. *U.S. v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) ("[W]e hold that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions."). Thus, the crux of plaintiff's argument is that defendants accessed social media services "without authorization" under 18 U.S.C. § 1030.[1]

Plaintiff's "without authorization" argument focuses on defendants' alleged use of plaintiff's name and image in creating "forged" social media accounts (e.g. Facebook and Twitter). Plaintiff attempts to cast defendants' behavior as analogous to that of hacking[2] proscribed by the CFAA. Plaintiff's argument is unpersuasive in light of (1) *LVRC Holdings LLC v. Brekka*, (2) *United States v. Nosal*, and (3) the rule of lenity.

I. *LVRC Holdings LLC v. Brekka*

In *LVRC Holdings LLC v. Brekka*,[3] the Ninth Circuit held that "a person uses a computer 'without authorization' under [the CFAA] when the person has not received permission to use

[1] Plaintiff does not articulate a particular provision under the CFAA. However, for purposes of this analysis, this Court will assume that plaintiff seeks recovery under 18 U.S.C. § 1030(a)(2)(C), (a)(4), and/or (a)(5)(B) & (C).
[2] Plaintiff also casts defendants' conduct as trespass under false pretenses.
[3] In *Brekka*, defendant, as an employee of plaintiff, was given an administrative log-in to access company documents and information. During his employment, Brekka emailed company documents to his personal

the computer *for any purpose* (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." 581 F.3d at 1135 (emphasis added). The Court further provided that "a person who uses a computer 'without authorization' has no rights, limited or otherwise, to access the computer in question." *Brekka*, 581 F.3d at 1133. Despite this relatively bright-line rule, this Court is reluctant to use it as an absolute bar to plaintiff's claim. To begin, unlike in *Brekka*, defendants are not employees of Twitter or Facebook who initially used the service for purposes of employment. Rather, as plaintiff alleges, defendants' relationship with the social media websites was "forged . . . from the ground up," i.e., the defendants, as social media users, never were authorized because they breached the terms of use at the inception of the relationship. Likewise, this court doubts that even the *Brekka* Court would enforce its "without authorization" language to the extent implicated.[4] For example, if a hacker[5] targeted a United States governmental website for malicious purposes, such a hacker may be "authorized" to

---

computer. The Court found that Brekka was still employed by plaintiff when "he emailed the documents to himself" and thus, Brekka "had authorization to use the computer." 581 F.3d 1127, 1133 (9th Cir. 2009).

[4] First, in *Brekka*, the Court stated "[t]here is no dispute that if Brekka accessed LVRC's information on the LOAD website after he left the company . . . Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA." In so stating, the Court focused on Brekka's alleged use of the "cbrekka" log-in (i.e., use of cbrekka username and password), and not Brekka's alleged access of the website itself. Thus, the Court's own analysis ignored possible permissible website access and instead focused on impermissible use of log-in information. Second, the *Brekka* Court cited an earlier Ninth Circuit opinion, *Theofel v. Farey-Jones*, to support its finding that "there is no dispute that Brekka had permission to access the computer." 581 F.3d at 1133 (citing *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2003). In *Theofel*, the Court discussed plaintiff's claim under the Stored Communications Act, 18 USC 2701 et seq. in terms of common law trespass. *Theofel*, 359 F.3d at 1072. The *Theofel* Court provided multiple examples of unauthorized access, e.g., a "busybody who gets permission to come inside by posing as a meter reader" and a "police officer who, invited into a home, conceals a recording device for the media." 359 F.3d at 1073. To the extent that *Brekka* relies on *Theofel*, the court appears receptive to a trespass scenario analogous to that alleged in plaintiff's complaint (i.e., defendants' posed as plaintiff to gain access to social media websites).

[5] In this example, the term "hacker" refers to "a person who uses his skill with computers to try to gain unauthorized access to computer files or networks." THE OXFORD-ENGLISH DICTIONARY Vol. VI, 1000 (2d ed. 2001); *see also* AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 787 (4th ed. 2000) (defining hacker as "one who uses programming skills to gain illegal access to a computer network or file.").

access the website under *Brekka* because many governmental websites are open to the public.[6] In other words, if interpreted strictly, *Brekka* could preclude CFAA application of "without authorization" to hackers who breach governmental websites that are open to the public.[7] For the same reason, strict adherence to *Brekka*'s bright-line rule outside of the employment context appears to be in conflict with the underlying legislative purpose.[8]

II. *United States v. Nosal*

In *United States v. Nosal*,[9] the Court in dicta,[10] found that "without authorization would apply to outside hackers (individuals who have *no authorized access* to the computer at all)." 676

[6] *See, e.g.*, United States Central Intelligence Agency, https://www.cia.gov/about-cia/site-policies/ (last visited Sep. 18, 2013) ("information presented on this Web site is considered public information and may be distributed or copied freely . . . ."); United States National Security Agency, http://www.nsa.gov/terms_of_use.shtml#security (last visited Sep. 18, 2013) ("The National Security Agency Web site (NSA.gov) is provided as a public service by the National Security Agency."); United States Department of Defense, http://www.defense.gov/landing/privacy.aspx (last visited Sep. 18, 2013) ("Information presented on this website is considered public . . . .").

[7] *See. e.g., Southwest Airlines Co. v. BoardFirst, L.L.C.*, 2007 WL 4823761, at *14 (N.D. Tex. 2004) ("[I]t is at least arguable here that [defendant's] access of the Southwest website is not at odds with the site's intended function; after all, the site is designed to allow users to obtain boarding passes for Southwest flights via the computer. In no sense can [defendant] be considered an 'outside hacker [ ] who break[s] into a computer' given that southwest.com is a publicly available website that anyone can access and use.").

[8] In Senate Report 104-357, the Senate Judiciary Committee stated that the purpose of the Leahy-Kyl-Grassley amendment was to "strengthen [the CFAA], by closing gaps in the law . . . ." S. REP. NO. 104-357, at 3 (1996), *reprinted* in 1996 WL 492169. This Report, in discussing coverage omissions, referenced the 1994 intrusion into the Griffiss Air Force Base in New York by a 16-year-old hacker based out of the United Kingdom and the 1996 Justice Department investigation of an Argentinian man who had broken into Harvard University's computers from Buenos Aires and used those computers as a staging ground to hack into other computer sites. *Id*. at 4-5. At least as to the Harvard example, it is plausible that the hacker's initial access could have been permitted under *Brekka* in modern times through Harvard's public website. *See* Harvard University, www.harvard.edu/ (last visited Sep. 18, 2013). In Senate Report 99-432, the Senate Judiciary Committee, in emphasizing the risk of computer crime, discussed the "414 Gang" who broke into the computer system at Memorial Sloan-Kettering Cancer Center in New York and gained access to the radiation treatment records of 6,000 past and present cancer patients. S. REP. NO. 99-432, at 2-3 (1986), *reprinted* in 1986 U.S.C.C.A.N. 2479, 2481. Memorial Sloan-Kettering Cancer Center now has a public website with a patient login portal. *See* Memorial Sloanj-Kettering Cancer Center, http://www.mskcc.org/ (last visited Sep. 18, 2013). Thus, under both Senate Reports, strict adherence to *Brekka* outside of the employment context appears to be in conflict with legislative intent.

[9] In *Nosal*, defendant, a former employee of Korn/Ferry, encouraged some of his former colleagues to transfer company documents and information to him. At the time, defendant's former colleagues were authorized to access the database, but were prohibited from disclosing the confidential information. 676 F.3d at 856. Defendant was charged with aiding and abetting his former colleagues in exceeding their authorized access with intent to defraud. *Id*.

[10] In *Nosal*, the Ninth Circuit reviewed Nosal's conviction under 18 U.S.C. 1030(a)(4) for aiding and abetting the Korn/Ferry employees in "exceed[ing their] authorized access" with intent to defraud. 676 F.3d at 856. Thus, the Ninth Circuit's discussion beyond "exceeding authorized access" was not essential to the decision. *See* Black's Law

F.3d at 858 (internal quotation marks omitted) (emphasis added). In contrast, the Court found that "exceeds authorized access would apply to inside hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." *Id*. (internal quotation marks omitted). The Court further provided that "hacking" colloquially refers to "someone who's authorized to access only certain data or files but accesses unauthorized data or files." *Id*. at 856-57. Unfortunately, the Court's colloquial definition provides little insight as to "outside hackers" because "hackers," by definition, lack authorized access.[11] However, the Court, in affirming the district court's dismissal of the claim, discussed numerous forms of relevant online conduct that it was unwilling to criminalize. Of these examples, many dealt with plaintiff's "trespass under false pretenses" scenario. The Court found that "lying on social media websites is common: People shave years off their age, add inches to their height and drop pounds from their weight." 676 F.3d at 862. The Court referenced *United States v. Drew*, to combat the notion that the government could be trusted to not "prosecute minor violations." *Id*. (citing 259 F.R.D. 449 (C.D. Cal. 2009). In *Drew*, a mother posed as a 16-year old boy ("Josh Evans") and cyber-bullied her daughter's classmate who ultimately committed suicide. 259 F.R.D. at 452. Although Drew's "Josh Evans" profile was fictitious, it did include "a photograph of a boy

---

Dictionary 519 (9th ed. 2009) (defining judicial dictum as "[a]n opinion by a court on a question that is directly involved, briefed, and argued by counsel, and even passed on by the court, but that is not essential to the decision"); *see also Weingand v. Harland Financial Solutions, Inc.*, 2012 WL 2327660, at *3 (June 19, 2012) ("[A]lthough Nosal clearly precluded applying the CFAA to violating restrictions on use, it did not preclude applying the CFAA to rules regarding access.").

[11] The term "authorization" is potentially subject to varying degrees of technical interpretation. For example, in *United States v. Morris*, the Second Circuit affirmed the criminal conviction of a defendant graduate student who used his access to a university's computer system to upload malware. 928 F.2d 504, 511 (2d Cir. 1991). Defendant Morris argued that his access was "authorized" because his worm only gained access to the other computers by virtue of their configurations and to the extent that defendant's worm circumvented passwords, it still only accessed the other computers in the manner to which they had been configured to be accessed. The Court rejected this argument, finding "Morris did not use either of those features in any way related to their intended function." 928 F.2d at 510; *cf. EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n. 10 (1st Cir. 2001) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven elusive."). The Ninth Circuit cited *Morris* for the proposition that "authorization" is of common usage. *Brekka*, 581 F.3d at 1132 (citing *Morris*, 928 F.2d at 511).

without that boy's knowledge or consent." *Id*. *Nosal*'s extensive discussion of "lying on social media websites" and its subsequent disapproval of prosecution under *Drew*, indicate that the Ninth Circuit is unwilling to recognize plaintiff's claim under the CFAA.

III. The Rule of Lenity

The term "authorization" is not defined in the CFAA. *Brekka*, 581 F.3d at 1132. In *Brekka*, the Ninth Circuit interpreted "authorization" narrowly and found the CFAA inapplicable to employee breach of loyalty scenarios. 581 F.3d at 1133; *but see International Airport Centers, LLC v. Citrin*, 440 F.3d 418, 419 (7th Cir. 2006) (interpreting the CFAA to recognize employee breach of loyalty as "without authorization"). In adhering to its narrow interpretation, the Ninth Circuit stated "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *Brekka*, 581 F.3d at 1134 (internal quotation marks omitted) (internal citations omitted); *cf*. *Nosal*, 676 F.3d at 863 (finding that a "narrower interpretation" of "exceeding authorized access" was "a more sensible reading of the text and legislative history").

As in both *Brekka* and *Nosal*, the rule of lenity precludes CFAA application as to defendants' alleged conduct. Under the rule of lenity, "penal laws [are] . . . to be construed strictly." *Nosal*, 676 F.3d at 863 (quoting *United States v. Wiltberger*, 18 U.S. 76, 88 (1820)) (internal quotation marks omitted). As stated in *Nosal*:

> We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals. [B]ecause of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity. If there is any doubt about whether Congress intended [the CFAA] to prohibit the conduct in which [defendants] engaged, then we must choose the interpretation least likely to impose penalties unintended by Congress.

Id. (internal citations omitted) (internal quotation marks omitted). The CFAA's focus is "on hacking" rather than the creation of a "sweeping internet-policing mandate." *Nosal*, 676 F.3d at 859. This court cannot fail "to consider the effect on millions of ordinary citizens caused by" recognizing plaintiff's claim. *Id*. at 863. Plaintiff alleges that defendants created false social media profiles in his name and likeness. Yet, as indicated in *Nosal*, "lying on social media websites is common." *Id*. at 862. For example, in June 2011, Facebook predicted that approximately 83 million of 855 million active users were duplicates, false or undesirable.[12] Twitter is also thought to have a large number of "fake" accounts.[13] More recently, police departments have taken to creating false profiles for the purpose of law enforcement.[14] Were this court to "adopt the [plaintiff's] proposed [argument], millions of unsuspecting individuals would find that they are engaging in criminal conduct," in addition to any civil liability. *Nosal*, 676 F.3d at 859. This Court "must choose the interpretation [of "authorization"] least likely to impose penalties unintended by Congress." *Id*. (quoting *United States v. Cabaccang*, 332 F.3d 622, 635 n. 22 (9th Cir. 2003) (internal quotations omitted)). Accordingly, this Court finds that the rule of lenity precludes application of the CFAA ("access without authorization") to defendants' alleged creation of fake social media profiles in violation of social media websites terms of use.

---

[12] Somini Sengupta, *Facebook's False Faces Undermine its Credibility*, N.Y. Times, Nov. 12, 2012, http://www.nytimes.com/2012/11/13/technology/false-posts-on-facebook-undermine-its-credibility.html.

[13] *See, e.g.*, Nicole Perlroth, *Researchers Call Out Twitter Celebrities with Suspicious Followings*, N.Y. Times, Apr. 25, 2013, http://bits.blogs.nytimes.com/2013/04/25/researchers-call-out-twitter-celebrities-with-suspicious-followings/?_r=0 ("fake Twitter followers offer potential for a $40 million to $360 million business."); Caitlin Moore, *Fake Twitter: The parody accounts to lighten up your news stream*, WASH. POST, Mar. 6, 2012, http://www.washingtonpost.com/blogs/arts-post/post/fake-twitter-the-parody-accounts-to-lighten-up-your-news-stream/2012/03/01/gIQALpiptR_blog.html ("Twitter allows untruths and parody to flourish with fake accounts . . . ."); Ashley Parker, *Fake Twitter Accounts Get Real Laughs*, N.Y. Times, Feb. 9, 2011, http://www.nytimes.com/2011/02/10/us/politics/10fake-twitter.html ("Fake Twitter personalities mock actors like Chuck Norris and world leaders like President Hosni Mubarak . . . .").

[14] *See, e.g.*, Heather Kelly, *Police embrace social media as crime-fighting tool*, CNN, Aug. 20, 2012, http://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html ("A more controversial approach to getting information . . . creating fake profiles to befriend suspects.").

CONCLUSION

For these reasons, Judge Coffin's F & R (#27) and (#29) are ADOPTED. Defendant Gary Hall's motion to dismiss for lack of subject matter jurisdiction (#14) is GRANTED and defendant S.A.'s motion for entry of a limited judgment and injunction (#25) is DENIED.

IT IS SO ORDERED.

DATED this 26th day of September, 2013.

_____s/ Michael J. McShane_____
Michael J. McShane
United States District Judge